**Lab Report**

**Lab Completed: Using Spear Phishing to Target an Organization**

**Objective:** Complete the lab presented. Using your textbook, the written lab, and the hands-on activity, use the lab report to demonstrate understanding of the concept presented.

**Part 1: Lab Activity**

Directions: Complete the lab assigned in Netlab. Take 2 screenshots (or more) that demonstrate completion of the lab. Answer the following:

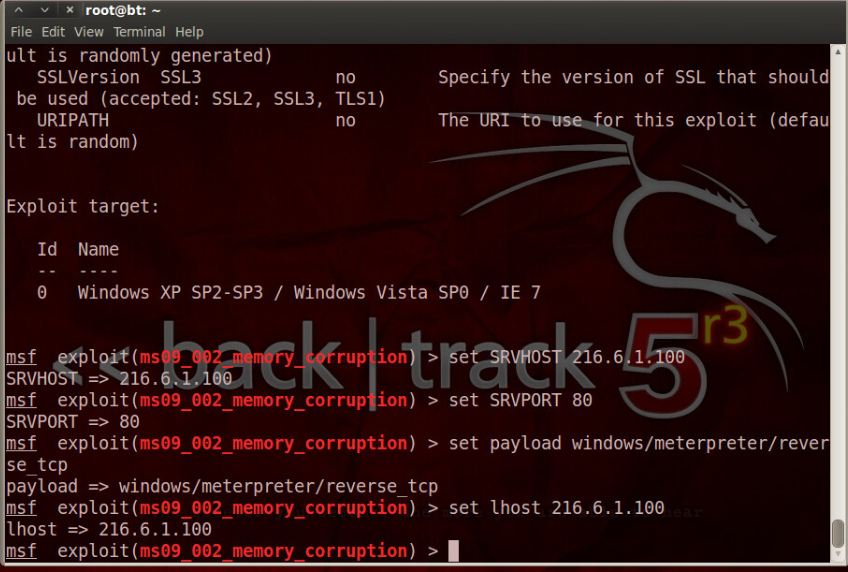
**Q1:** Provide a synthesis of the activity you completed in your own words.

We were sending a meterpreter payload that established a reverse tcp shell. This payload took advantage of a vulnerability in Microsoft Explorer and was cleverly masked as a link in an email about relief from the “IRS”. After establishing a shell, we got a list of currently running processes and dumped the password hashes from the victim machine.

**Q2:** Provide 2 screenshots that demonstrate lab completion. For each screenshot, include 1-2 sentences explaining what the screenshot is demonstrating.



This is a screenshot from the beginning of the lab. Here I was just exploring various Internet Explorer vulnerabilities in the metasploit database.



Here we had decided on an exploit and proceeded to set the server host, server port, payload, and local host variables.

**Part 2: Critical Thinking**

**Directions**: Complete the following questions. Provide an explanation of your reasoning for each answer.

The answers should address the lab you just completed.

Suggested length for Part 2: 1-2 pages

**Q1**: What vulnerability(s) are demonstrated or found in this lab? Vulnerabilities may occur during the lab as part of the lab activity.

There was the actual vulnerability in the browser here, but I would say there were also a couple of others. I think the fact that this email even made it through to someone’s inbox could be considered a vulnerability in the email filter, and the fact that an employee chose to open it represents a human vulnerability.

**Q2:** How might this (these) attack(s) be utilized during a penetration test?

If you needed to gain a foothold on the intranet of an organization and are having trouble compromising the organization externally, you could target someone internally with a specially crafted payload like this one and then pivot from there.

**Q3:** Explain your reasoning as to what phase of the attacker methodology this lab falls under.

Infiltration and Escalation + Exfiltration. They are using information about the employee (i.e. browser and operating system version) to craft a malicious payload that then grants them access to that company’s environment. After establishing a shell, we also get environment information, a list of running processes, and do a hashdump, which is the exfiltration part of this lab.

**Q4:** Research how the attack(s) in this lab can be mitigated or prevented. Cite any sources used. (APA)

First, I think a more robust email filter is in order. This email should have never been delivered with the spoofed email address and obviously masked link leading to a malicious payload.

The operating system could be updated to a more recent version that includes security patches to prevent this exploit from working.

The employee(s) at this company could use a refresher on best security practices when receiving emails with external links/files/etc.

**Q5:** What ethical or potentially problematic issues should a penetration tester consider if they plan on implementing this (these) attack(s) by exploiting a vulnerability?

Am I allowed to target this employee per the rules of engagement? Could this create outbound traffic that could potentially be leveraged by an actual threat actor? Will this exploit exfiltrate any data or trade secrets that are not to be accessed?